ISSN 2047-3338

Performance Analysis of WiMax Physical Layer under Scrambling Security Threat Using MATLAB Simulation

Muhammad Aamer[1], Abdul Maalik[2] and M. Junaid Arshad[3]
[1,2]Department of Electronics, The University of Lahore, Pakistan
[3]Department of Computer Science and Engineering, UET, Lahore-Pakistan
[1]maamer.saif@gmail.com

***Abstract*– The main focus of this research work is on Physical layer (PHY) of the WiMAX. Scrambling and Jamming are two security threats which can occur at physical layer of the WiMAX network. In WiMAX environment jamming and scrambling threats can be destroyed the Communication. Scrambling is a type of jamming and it is a risk to WiMAX security and has great impact as it affects burst of data effecting one or more frames for short period, therefore it cannot be detected easily. As scrambling effect on specific frames so if it affects control and information frames then there should be a great problem in WiMAX Network. Scrambling can also be generated naturally that is why this threat is also important in the WiMAX network. Due to all these scrambling issues, before implementing the WiMAX architecture, we will introduce our scrambling in the WiMAX system then using MATLAB simulation check out its effect on this WiMAX system. In the end we add our descrambler module at the receiver side that is used to discard the scrambling.**

***Index Terms*– WiMAX, Orthogonal Frequency Division Multiplexing, PHY, MAC, Scrambling and MATLAB**

I. INTRODUCTION

WITH emerging technologies and higher data rate requirements new ways of communications are being developed. These developments are both in wired and wireless communications. Different technologies are introduced like Wi-Fi, Bluetooth, and WiMAX etc. Wi-Fi is used to provide wireless internet to the users but due to its limited range it can cover certain meters only. So, to increase the range of wireless internet access, the concept of WiMAX is introduced.

WiMAX offers high data rates, sophisticated, protected long range broadband services. It also provides a cellular backhaul and helps creating Wi-Fi hotspots [1]. In rural areas and disaster areas which are affected due to flood and earthquake etc., it is difficult to established wired infrastructure then engineers and scientist thinks there should be a replacement of this so, work on WiMAX is start. When work start on it scientist and engineers made different standard for fix broadband services and for mobile services. For fixed WiMAX 802.16d is used and for mobile WiMAX 802.16e is using [2].

Initially work on WiMAX standards has been started in 1999 by the WiMAX forum and the first standard which is made by this forum is 802.16-2001 and it is accepted in December 2001[3]. 10-66 GHz frequency spectrum is used for 802.16-2001 standard of WiMAX and it is designed for 72 Mbps data rates in which point to point communication is done and also point to multipoint communication can be done. Due to Line of site limitation this standard was not successful. Due to these limitations, a modified standard, IEEE 802.16a, is made by this forum and this came in 2003 followed by its two variants 802.16b and 802.16c then 802.16d for fix and 802.16e for mobile came [4]. Base Stations (BSs) and Mobile Stations (MSs) are present there in WiMAX network for communication. The connection between subscribers and mobile stations is offered by Base Stations. In the WiMAX network subscriber is distinct by user and mobile stations and base station both play the role of system. Environment of simple WiMAX can be shown as in Fig. 1 [4].

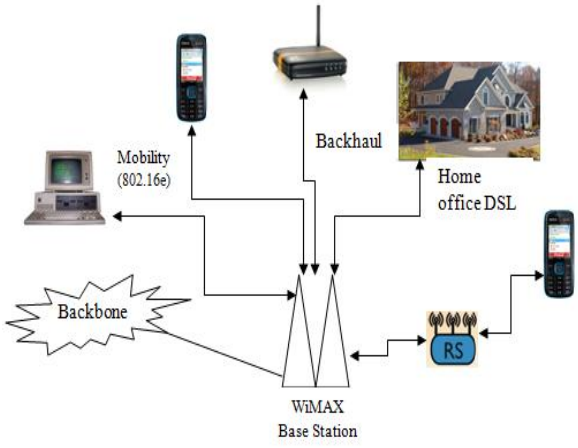

Fig. 1: Overview of WiMAX Environment

II. PROBLEM STATEMENT/MOTIVATION

Physical Layer of WiMAX has some threats like Scrambling and jamming [5]. But there are no sufficient measures taken to cater with threats associated to PHY layer of WiMAX so, the PHY layer of WiMAX is endangered with the threats like jamming and scrambling.

Channel capacity requests and their responses are some examples of time sensitive messages which can lead to a disaster if scrambling is introduced by the attacker. Scenarios where Time Division Multiplexing is implemented, scrambling can cause frequent retransmissions by effecting intended user time slots, resulting in wastage of bandwidth. Intensions of this type of attack are to reduce the bandwidth of competitive user and increasing attacker's data processing as well as bandwidth. Attacker may sometime find difficult to introduce scrambling but professionals can solve these technical complications with ease.

Unlike jamming, scrambling only effect short burst of data and therefore it is difficult to identify it only the irregularities in victim's data can spot scrambling. Sometimes usual channel noise can also cause scrambling. Therefore it is not possible to distinguish between scrambling caused by the attacker or caused by the channel noise so measures should be taken to counter it.

We want that our data should be secure and not even single person or user can access it without our permission. This is also a main purpose of WiMAX PHY Layer security. In this research work PHY layer and its threat is considered. When we talk about security for WiMAX it means security for each layer of WiMAX layers.

In this research work scrambling will be observed in detail. It is type of jamming. The main purpose of scramblers to affect the normal operation of the network so, they select control and management information and then scramble it. Scrambling can also be generated naturally that is why this threat is also important in the WiMAX architecture. We will do Simulation to see the performance of the WiMAX system under scrambling environment. And MATLAB tool is used for this purpose. PHY Layer's main threat are jamming and scrambling which is also most important for military and personal application. Now technology reaches to the regular users. Signal generators are available to generate signals in IEEE 802.16 spectrum. Basically our research work revolves around the simulation of the physical layer of WiMAX and threat which associated with it. Simulation approach is easy but practical result may be somewhat different then simulation result.

But simulation gives some idea about the scrambling scenario. The advantage of simulation over practical is that consistent setup of instrument is not required. In simulation parameters can be changed and different results can be generated as well as analyzed.

III. OBJECTIVES AND SCOPE

Some objectives of the research are:

- The primary goal of this research is that how WiMAX system responds under scrambling as well as without scrambling.
- How to descramble data in WiMAX system under scrambling.
- The main idea of our research work is to simulate the physical layer of WiMAX and introduce scrambling in the system and then add modules to descramble it

IV. PROPOSED METHODOLOGY

With the passage of time, use of the Internet is increasing and the vendor wants to provide best services to end users. Vendors are providing both wired and wireless internet to the users. Now a day's end users prefer wireless internet because they can easily move from one place to other using internet so vendors try to provide this facility to the end users. In wireless different technologies are using like Wi-Fi, Bluetooth and WiMAX. Because end users want mobility, high bandwidth and QOS so vendor prefers WiMAX. In wireless communication security is very important so for confined communication it is very important. Everybody knows that communication is exchange information between two person or source and destination node but according to our point of view it is protected information which is send from source node to end node.

But there are also different issues which should be solving first then it provide to the end users. In our thesis we choose one issue which is security related at physical layer that is scrambling. Studying the protocol architecture of WiMAX we see that security layer is present in MAC layer so intruder can easily change or destroy the information which is passing through PHY Layer, because at PHY Layer data is present in the form of binary. So, we checked PHY Layer in MATLAB using simulation. In Fig. 2, we show an overview of the WiMAX architecture.

In Fig. 3, we have shown the proposed system design that we have implemented at Physical Layer of WiMAX for seeing the effect of scrambling on the system.

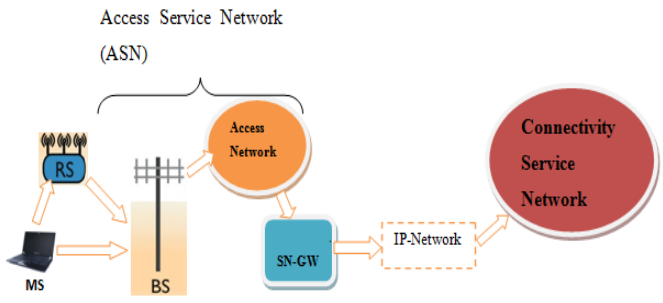

Fig. 2: Overview of WiMAX Architecture

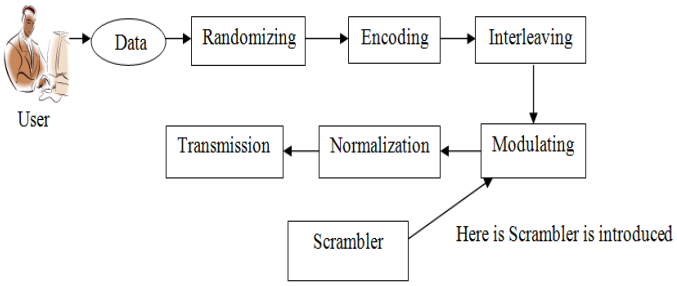

Fig. 3: Propose Systems Design

MATLAB is the basis tool which we will use for simulation because it is easy to use and the work which we want to do, easily implement using it. Because it provide some predefined blocks which do my work user easier. These blocks are DATA, RANDOMIZER, ENCODER, INTERLEAVER, MODULATOR, NORMALIZER, and TRANSMITTER.

Manually we introduce our scrambler in the WiMAX Physical Layer model and then Analysis the WiMAX Physical Layer under these scrambling and explain our views and then transmit it. Then at the receiver side we implement our descrambler according to the scrambling which we introduced in previous step.

In the end we see that our input and output data is same which means we are successful but there are some issue which is also relate to performance point of view that can be SNR with respect to BER So, we also check the SNR effect w. r. t. BER when Scrambler is introduced in the system and when not introduced in the system.

Data

In this block we get integer data from workspace or this integer data can also be getting from M-File. Then by using Integer to Bit Convertor block that is present inside the Data block, we convert this data into bits and generate output.

Randomizer

When bits are generated at the output of Data block then Randomizer Block start their work. It is the very first process which is done at physical layer when data comes from upper layers. It randomizes all data even it come from uploading or even downloading. It randomizes all data bit by bit. For this purpose there is PN Sequence Generator Block is present inside the Randomizer block which generates pseudorandom binary numbers by using Linear Feedback Shift Register.

Encoding

In this block randomized data is encoded by using R-S (Reed Solomon) Encoder. Like hamming code and other error correction codes R-S are also codes which are used to detect and correct multiple symbol errors.

Interleaver

This block work like randomizer block but in this block bits state don't disturb it remains same. It operates with the place of bits. Before transmission the symbols it is coded in time and the data that come to Interleaver it is randomize into two variations. First variation, contiguous bits are mapped onto a non-contiguous sub carriers. In the Second variation we mapped the contiguous coded bits onto less or more important bits of group. According to OFDM symbol bits, all encoded data are interleaved in the Interleaver. These coded bits depend upon the modulation scheme.

The WiMAX 802.1 6e defines two variations for the Interleaver [7].

The 1st variation is defined **by** the formula:

mk = (Ncbps/ **12) *** mod (k, 12) + floor (k/ **12)**

The 2nd variation is defined **by** the formula:

s = ceil (Ncpc/2)

jk = s x floor (mk / s) + (ink + Ncbps – floor (2 xmk / Ncbps)) mod (s)

Where:

Ncpc = Number of coded bits per carrier

Ncbps= Number of coded bits per symbol

k = index of coded bits before first variation

mk =Index of coded bits after first variation

jk = Index of coded bits after second variation

Modulator

In this block we implement our scrambler and modulations technique which scrambled data according to modulation technique. The scrambling data must be scalar. Our main purpose to reduce the length of data which is consists of 0s and 1s in the transmitted signal. For example Q = [1 0 0 1 1 0 0 1] and Q = [0 -3 -4 -7] both are same polynomials Q (z-1) = $1+z^{-3}+z^{-4}+z^{-7}$

If there are N integers then the there must be integers between 0 and N-1. Scramble polynomial and the length of vector of these integers should be same. The process of scrambling is shown in Fig. 4.

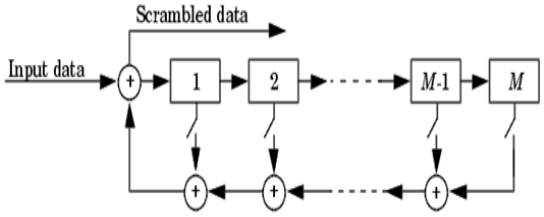

Fig. 4: Process of Scrambling Data

Normalizer

In this block we simply conjugate the input which is getting from previous block that is modulator and then multiply the output of conjugate with the gain of 1/sqrt (2).

Transmitter

It is most important block of sender side in which AWGN channel is used. The main purpose of this channel is to add white Gaussian Noise in the real and complex signal. For producing real output for real input signal it adds real Gaussian Noise and for complex output signal it adds complex Gaussian Noise in the input signal.

V. SIMULATION AND ANALYSIS

In this section, first we show the basic simulation model (Fig. 5) which we implement in the MATLAB. Then we will show the blocks which are using in this simulation model and also define some description which will be related to these blocks.

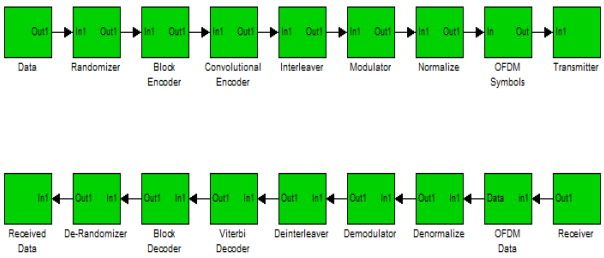

Fig. 5: Simulation Model

Blocks Description:

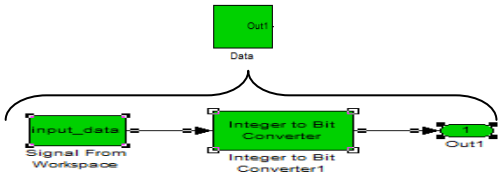

Fig. 6: Data Block

In this block (Fig. 6), we get integer data from workspace or this integer data can also be getting from M-File. Then by using Integer to Bit Convertor block that is present inside the Data block, we convert this data into bits and generate output.

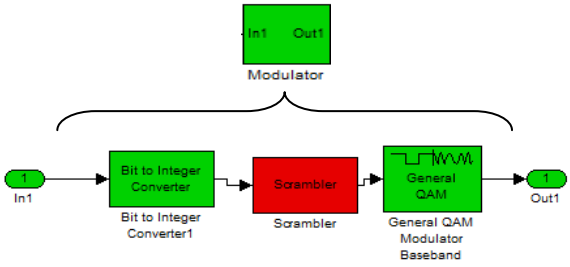

Fig. 7: Modulator Block

In this block (Fig. 7), we implement our scrambler and modulations technique which scrambled data according to modulation technique.

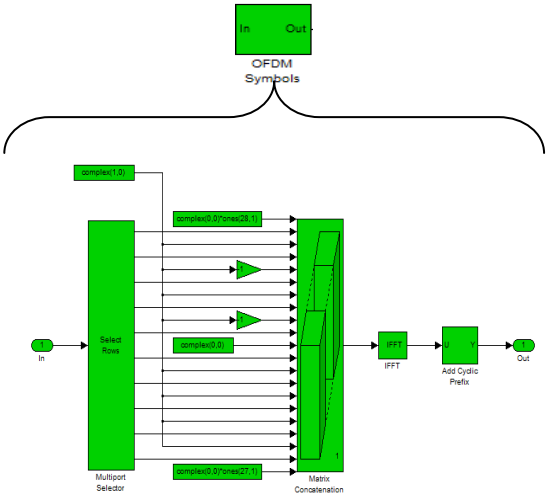

Fig. 8: OFDM Block

In OFDM block (Fig. 8), multi-carrier modulation technique is used to transfer signal using multiple carriers.

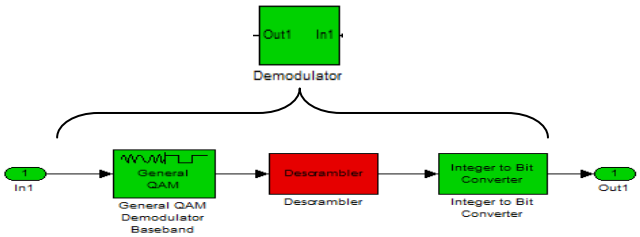

Fig. 9: De-modulator Block

In the end we will show the de-modulator block (Fig. 9) because all other blocks work reverse of the transmitter side. This is also reverse but we want to show it in this work.

The simulation results are shown in the following figures. In the Fig. 10, firstly we showed data inputs and outputs by introducing the scrambler. We see that there is lot of difference between inputs and outputs.

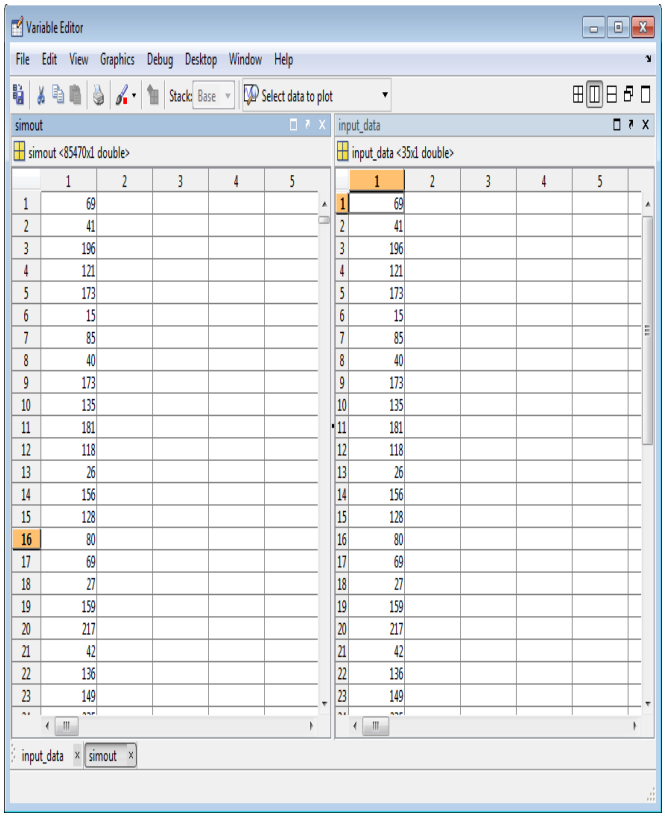

Fig. 10: Difference b/w Data Inputs and Outputs

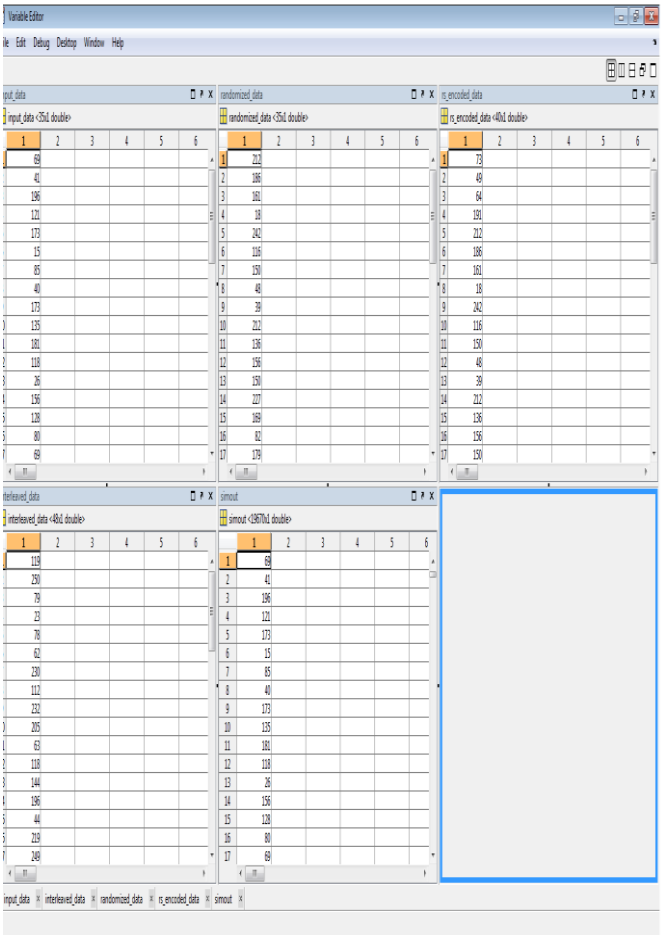

Fig. 11: No Difference b/w Data I/O when Descrambler introduced

Then introduced descrambler in the model and showed the input and output data in the Fig. 11, we see that input and output data is same and out descrambler is working very well.

The detail description of above data is shown in Fig. 12 in which randomized, encoded and interleaving data are also shown.

In the end we also plot graph between inputs and outputs differences w. r. t. different SNR values which is shown in Fig. 13 and Fig. 14, and also calculate the bit error b/w input data and output data by using the formula in MATLAB, i.e., [Number, Ratio] = biterr (input_data, simout). This formula computes no. of bit errors and bit rate also.

Some other observations also are taken in which power is taken as a constant and vary the SNR and take different readings and also plot the graphs as shown in the Fig. 15 and Fig. 16.

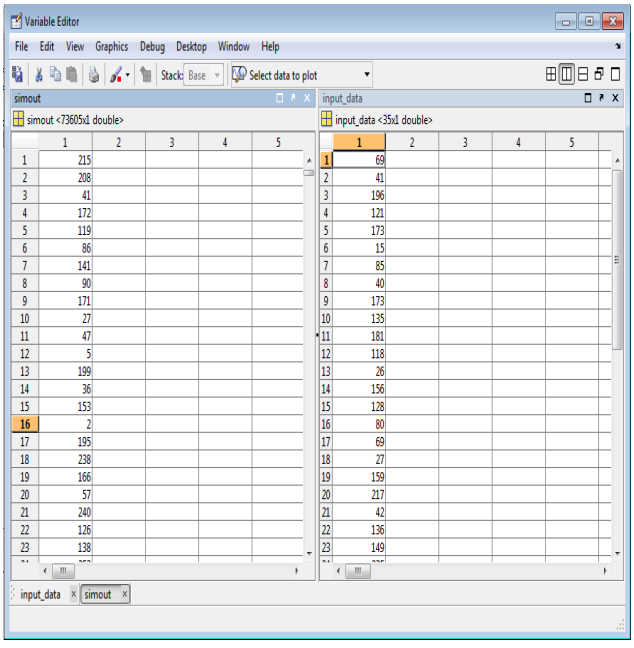

Fig. 12: Detail Description of Data

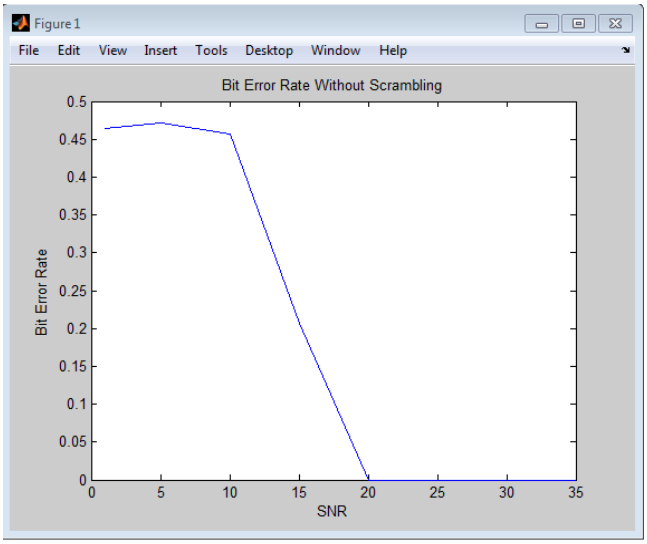

Fig. 13: Difference b/w Data I/O without Scrambler

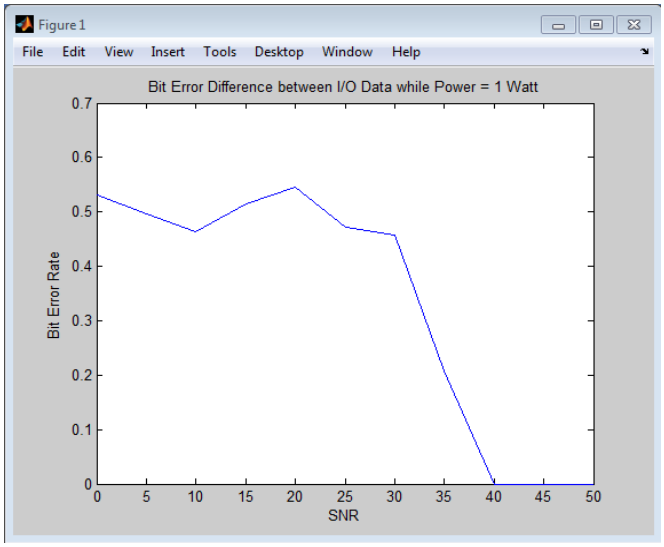

Fig. 15: BER Difference While Power = 1 watt

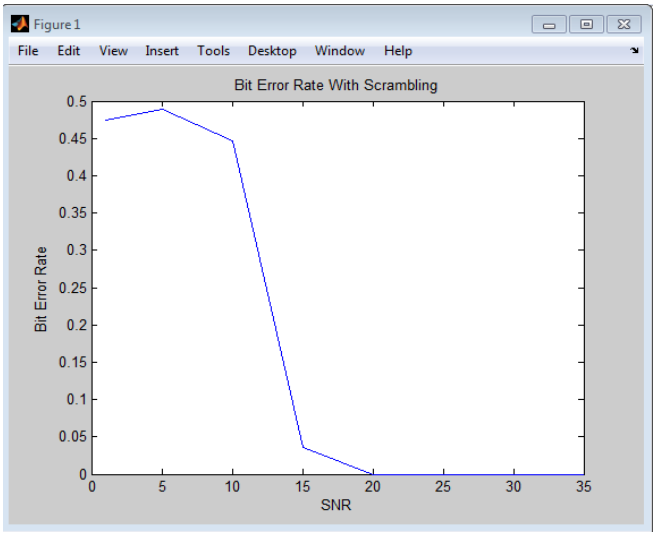

Fig. 14: Difference b/w Data I/O with Scrambler

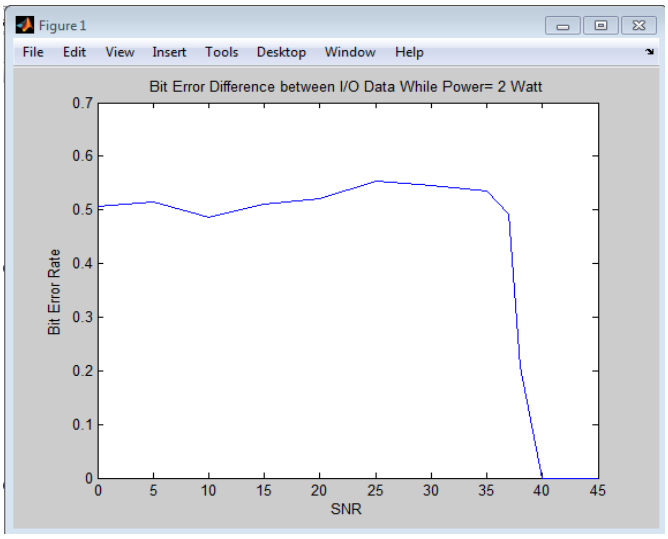

Fig. 16: BER Difference While Power = 2 watt

VI. CONCLUSION AND FUTURE RECOMMENDATIONS

Scrambling as discussed in the problem statement and motivation section has successfully been countered and analyzed. We implemented Physical Layer model of WiMAX in MATLAB effectively. We take different tests and checked the performance. The results that we got from simulation, define that system is best under descrambling. Firstly we introduced the scrambler in our system and observed its results; and generated graphs between inputs and output so we have implemented descrambler module for acquiring the required output. Also we have determined the bit error rates for different values of SNR under scrambling and after descrambling. We concluded that system performs better and has low bit error rates under descrambler model as compared to model in which we introduced scrambling.

Future Recommendations:

It is suggested that following features should be included to enhance the simulation model. It will help in improving security and performance of WiMAX system.

- Antennas may be used for the transmission to show the effects of jamming.
- Jamming of signals then can be removed by implementing the solutions
- The simulation model can be extended to implement the whole WiMAX system and then analysis of its performance can be observed.

REFERENCES

[1]. Sunil .N. Katkar, Prof. Ashwini S. Katkar ,Prof. Dattatray S. Bade "Performance Evaluation of IEEE 806.16e (Mobile WiMAX) in OFDM Physical Layer" IJERA ISSN : 2248-9622 VNCET- 30 Mar 12.

[2]. J. G. Andrews, A. Ghosh and R. Muhamed, "Fundamentals of WiMAX Understanding Broadband Wireless Networking," Prentice-Hall, Upper Saddle River, 2007.

[3]. Barbeau, Michel; "WiMAX/802.16 Threat Analysis," Association for Computing Machinery, pp., Oct.2005

[4]. Anmar Hamid Hameed, Salama A. Mostafa, Mazin Abed Mohammed. Simulation and Evaluation of WIMAX Handover over Homogeneous and Heterogeneous Networks. American Journal of Networks and Communications. Vol. 2, No. 3, 2013, pp. 73-80.

[5]. M. E.-H. A. E.-H. Mahmoud Narsreldin, Heba Aslan, "WiMAX security," in 22nd International Conference on Advanced Information Networking and Applications, 2008, pp. 1335–1340.

[6]. W. C. Taeshik Shon, "An analysis of mobile WiMAX security: Vulnerabilities and solutions," Lecture notes in computer science, Springer, 2007.

[7]. R. Poisel, "Modern communications jamming principles and techniques," Artech House Publishers, 2003.

[8]. A. A. Ayesha Altaf, Rabia Sirhindi, "A novel approach against dos attacks in WiMAX authentication using visual cryptography," in The Second International Conference on Emerging Security Information Systems and Technologies, securware, Cap Esterel, France, 2008.

[9]. S. Haykin and M. Moher, "Modern Wireless Communication," Prentice-Hall, Upper Saddle River, 2005.

[10]. M. Raya, J.-P. Hubaux, and I. Aad. Domino: A system to detect greedy behavior in IEEE 802.11 hotspots. In Proceedings of the 2nd International Conference on Mobile Systems, Applications and Service (MobiSys), pages 84–97, Boston - MA, 2004.

[11]. http://en.wikipedia.org/wiki/Mail_delivery_by_animal (Last Visited 10 Sep 2013).

[12]. http://en.wikipedia.org/wiki/Invention_of_the_telephone (Last Visited 10 Sep 2013).

[13]. Deepak Pareek, "The Business of WiMAX," John Wiley & Sons Ltd, 2006.

[14]. Yufei Wang; Qixin Wang; Zheng Zeng; Guanbo Zheng; Rong Zheng, "WiCop: Engineering WiFi Temporal White-Spaces for Safe Operations of Wireless Body Area Networks in Medical Applications," Real-Time Systems Symposium (RTSS), 2011 IEEE 32nd , pp.170,179, Nov. 29 2011-Dec. 2 2011

[15]. Jie Yuan; Ward, T.; Honarvar, S.; Tingting Chen; Thomas, J., "HMM-driven Smart White-space-aware Frame Control Protocol for coexistence of ZigBee and WiFi," Pervasive Computing and Communications Workshops (PERCOM Workshops), 2013 IEEE International Conference on, pp.348, 351, 18-22 March 2013.

[16]. Wenxian Li; Yanmin Zhu; Tian He, "WiBee: Building WiFi radio map with ZigBee sensor networks," INFOCOM, 2012 Proceedings IEEE, pp. 2926-2930, March 2012.

[17]. Chung-Hsin Liu; Shi-Wei Dai, "The Study for the Extension of Bluetooth Ring Network," Multimedia and Information Technology (MMIT), 2010 Second International Conference, Vol. 2, pp. 127-130, 24-25 April 2010.

[18]. Nasreldin, M.; Asian, H.; El-Hennawy, M.; El-Hennawy, A., "WiMax Security," Advanced Information Networking and Applications - Workshops, 2008. AINAW 2008. 22nd International Conference on, pp.1335, 1340, 25-28 March 2008

[19]. Jha, R.K.; Limkar, S.V.; Dalal, U.D., "Performance Analysis under the Influence of Jamming for WiMAX System," Emerging Applications of Information Technology (EAIT), 2011 Second International Conference on , pp.292,297, 19-20 Feb. 2011

[20]. Etemad, K., "Overview of mobile WiMAX technology and evolution," Communications Magazine, IEEE, vol.46, no.10, pp.31, 40, October 2008.

[21]. Pareit, Daan; Lannoo, Bart; Moerman, Ingrid; Demeester, Piet, "The History of WiMAX: A Complete Survey of the Evolution in Certification and Standardization for IEEE 802.16 and WiMAX," Communications Surveys & Tutorials, IEEE, Vol. 14, No. 4, pp.1183-1211, Fourth Quarter 2012.

[22]. Parsaee, G.; Yarali, A., "OFDMA for the 4th generation cellular networks," Electrical and Computer Engineering, 2004, Canadian Conference on, Vol. 4, pp. 2325-2330.

[23]. en.wikipedia.org/wiki/MathWorks (Last Visited 10 Sep 2013).

[24]. Patidar, M.; Dubey, R.; Jain, N.K.; Kulpariya, S., "Performance analysis of WiMAX 802.16e physical layer model," Wireless and Optical Communications Networks (WOCN), 2012 Ninth International Conference on, pp.1, 4, 20-22 Sept. 2012.